IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	CASE NO. 1:16-CR-00270
Plaintiff,	)	
	)	JUDGE SARA LIOI
-vs-	)	
	)	
LAUDEN A. SULLIVAN,	)	GOVERNMENT'S OPPOSITION TO
	)	DEFENDANT'S MOTION TO SUPPRESS
	)	
Defendant.	)	

Now comes the United States of America, by its counsel, Carole S. Rendon, United States Attorney, and Benedict S. Gullo, Assistant U.S. Attorney, who respectfully move this Court to deny Defendant's Motion to Suppress.

Respectfully submitted,

CAROLE S. RENDON
United States Attorney

By: /s/ Benedict S. Gullo

Benedict S. Gullo (NY: 3013570)
Assistant U.S. Attorney
Suite 400, U.S. Courthouse
801 West Superior Avenue
Cleveland, Ohio 44113–1852
Tel. No. (216) 622-3807
E-mail: benedict.gullo@usdoj.mil

FACTUAL BACKGROUND

A. "Website A"

The charges in this case arise from an investigation into a global online forum dedicated to the advertisement and distribution of child pornography through which registered users like Sullivan regularly advertised, distributed and accessed illegal child pornography. The scale of child sexual exploitation that occurred on the site was massive—it contained more than 150,000 total members who collectively engaged in tens of thousands of postings related to child pornography. The images and videos that were advertised, distributed, and accessed through the site were highly categorized according to the gender and age of the victims portrayed—including so-called "jailbait," "pre-teen," and "toddlers;" as well as the type of sexual activity depicted, including hardcore ("HC") and softcore ("SC") child pornography. The most postings to the site (more than 20,000 posts) were made within a subsection for "Pre-teen" videos dubbed "Girls HC," where hardcore pornographic images of pre-teen girls were advertised, distributed, and accessed. The site also contained forums for the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders used to abuse children, as well as methods and tactics offenders used to avoid law enforcement detection.

The site, referenced herein as "Website A," operated on the anonymous Tor network—which allows users to mask their actual IP addresses while accessing the Internet.[1] To access Tor, a user must install Tor software either by downloading an add-on to the user's web browser

[1] Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. Owed to its anonymizing properties, the Tor network has become a haven for criminal activity in general, and the online sexual exploitation of children in particular. See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds, WIRED MAGAZINE, December 30, 2014, *available at* https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/.

or by downloading the free "Tor browser bundle" available at www.torproject.org.[2] Use of Tor software masks the user's actual IP address, which could otherwise be used to identify a user, by bouncing user communications around a distributed network of relay computers (called "nodes") run by volunteers all around the world. Because of the way Tor routes communications through other computers, traditional IP-address-based identification techniques used by law enforcement agents investigating online crimes are not viable. When a user on Tor accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node IP address.

Within Tor, entire websites such as "Website A" can be set up as "hidden services." "Hidden services," like other websites, are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix "onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. Unlike an open Internet website, it is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

[2] Users may also access Tor through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of Tor.

The use of Tor also makes websites like "Website A" more difficult to find for users. Even after connecting to Tor, a user must know the exact web address of a site like "Website A" in order to access it. Accordingly, to find "Website A," a user had to first obtain the web address for it from another source—such as from other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing a Tor website like "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

While the FBI was able to view and document the substantial illicit activity taking place on "Website A," investigators faced a tremendous challenge to identify the site users engaging in the sexual exploitation of children through the site. Open-Internet, non-Tor websites generally have user IP address logs that can be used to locate and identify the site's users. In such cases, after the lawful seizure of a website whose users were engaging in unlawful activity, law enforcement could review those IP logs to determine the IP addresses of site users. Law enforcement agents could then perform a publicly available lookup to determine what Internet Service Provider ("ISP") owned the target IP address, and address a subpoena to that ISP to determine the user to which the IP address was assigned at a pertinent date and time. However, because "Website A" was a Tor website, any such logs of user activity contained only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Tor network to that actual user. Such IP address logs

therefore could not be used to locate and identify users of "Website A." Accordingly, for law enforcement to attain the sort of information normally available from public sources and through ordinary investigative means, the offenders' use of the Tor network necessitated a particular investigative strategy.

Acting on a tip from a foreign law enforcement agency as well as further FBI investigation, the FBI determined that the computer server that hosted "Website A" was located at a web-hosting facility in North Carolina. In February of 2015, FBI agents apprehended the administrator of "Website A" and seized the website from its web-hosting facility in North Carolina. Rather than merely shutting the site down—which would have allowed the users of the site to go unidentified and un-apprehended, the FBI interdicted the site and allowed it to continue to operate at a government facility located in the Eastern District of Virginia. The FBI operated "Website A" during a two-week period from February 20, 2015 to March 4, 2015. During that brief period, the FBI obtained court approval from the United States District Court for the Eastern District of Virginia to monitor site user's communications and to deploy a Network Investigative Technique ("NIT") on the site. The NIT was designed in order to attempt to identify registered site users anonymously engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation. (See Attachment A.)

As described in detail in the application for the warrant authorizing its use, the NIT consisted of computer instructions which, when downloaded (along with the other content of "Website A") by a registered user's computer, were designed to cause the user's computer to transmit a limited set of information—the computer's true IP address and other computer-related information—that would assist in identifying the computer used to access "Website A" and its

user. The search warrant authorized minimally invasive technique to be deployed when a registered user logged into "Website A" by entering a username and password, while the website was located in the Eastern District of Virginia.

B. Lauden Sullivan, "554422"

User "554422" created an account on "Website A" on January 21, 2015. From January 21, 2015 until the FBI shut down "Website A" on March 4, 2014, 554422 logged into the website for a total of 7.24 hours. 554422 logged into "Website A" from IP address 76.188.24.146.

Of note to the FBI, on March 1, 2015, "554422" accessed "Website A", and more specifically, the post entitled, "12yo and dog." The thumbnail images for this post depicted an approximately 10–12-year-old female, nude from the waist down. In the initial images, the female uses her hands to hold open her labia and display her vagina. As the thumbnail progresses, the juvenile female lays on her back with her legs spread apart, displaying her vagina. In some of the later images, a dog is seen atop the juvenile female, with one of the images showing the dog's muzzle near the vagina of the juvenile female.

On March 4, 2015, 554422 accessed a post under a thread titled "6yo girl masturbating with a toothbrush and gets fucked, with cum and sound." The original user posting the video wrote,

> This is one of the most lovely [sic] perverted videos I have seen for ages. A 6yo girl sitting on a toilet seat is masturbating with the back of a toothbrush. The guy starts to fuck her while she is masturbating then cums all over her pussy. Even though her pussy is covered with his sperm, she carries on masturbating using his cum as a lube.

The link shows a series of 12 thumbnail images from a video which depict an approximately 5–7-year-old prepubescent female, nude from the waist down, sitting on a toilet. The juvenile

female is shown rubbing her vagina with the back of a toothbrush, and an erect male penis is shown penetrating the girl's vagina. In the final two images, the girl's vagina is shown with what appears to be sperm all over her vagina and her pelvic area. The prepubescent girl continues to rub her vagina with the back of the toothbrush.

Finally, on March 4, 2015 user "554422" viewed the post entitled "12y Preteen Girl Wants 9y Boy Cock Inside Her Ass And Pussy." The post included a contact sheet, or preview image, with twenty images that depicted what appeared to be a prepubescent boy anally penetrating a female. After viewing the post and the preview image, user 554422 downloaded the preview image.

Using publicly available websites, the FBI determined that the above-referenced IP address used by 554422 was operated by the Internet Service Provider ("ISP") Time Warner. On March 11, 2015, an administrative subpoena/summons was served to Time Warner requesting information related to the user who was assigned IP address 76.188.24.146 on March 1, 2015. Per the information received from Time Warner, Lauden Sullivan, with an address of 1216 West Jackson Street, Painesville, Ohio 44077, was receiving internet service at that time. Time Warner's response also indicated the internet service was installed on June 25, 2014.

On January 19, 2016, the FBI applied for a search warrant to search and seize any evidence related to child exploitation at 1216 West Jackson Street, Painesville, Ohio 44077. The search warrant was issued by Magistrate Judge William H. Baughman Jr., here in the Northern District of Ohio. (See Attachment B).

On January 22, 2016, the FBI executed a search warrant at 1216 West Jackson Street, Painesville, Ohio 44077. The FBI recovered a computer from Sullivan's bedroom. In an interview conducted that same day, Sullivan admitted to accessing Tor on his computer, but he

denied possessing or viewing any child pornography on his computer. On Sullivan's computer, the FBI later found approximately 662 images and 145 videos of suspected child pornography. The forensic analysis of the computer showed activity on Sullivan's computer from January 4, 2015 through January 21, 2016—spanning a period in excess of one year.

On August 24, 2016, a two-count Indictment was filed against Sullivan in the Northern District of Ohio. Count 1 charges Sullivan with Receipt and Distribution of Child Pornography in violation of Title 18, United States Code, Section 2252(a)(2). Count 2 charges Sullivan with Possession of Child Pornography in violation of Title 18, United States Code, Section 2252A(a)(5)(B).

On August 31, 2016, Sullivan was arrested at his home by the FBI. During his transport to court to be processed and arraigned, and after being provided his Miranda warnings, Sullivan told an FBI agent, "I only looked at [Tor] one time." Sullivan made this comment when talking about what he was being charged with.

SEARCH WARRANT AUTHORIZING THE NIT

The 31-page NIT search warrant affidavit was sworn to by a veteran Federal Bureau of Investigation (FBI) agent with nineteen (19) years of federal law enforcement experience—with particular training and experience investigating child pornography and the sexual exploitation of children. It clearly and comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist law enforcement in identifying registered site users who were utilizing anonymizing technology to expose children to ongoing and pervasive sexual exploitation on a massive scale.

A. Technical and Legal Background of Investigation

In recognition of the technical and legal complexity of the investigation, the affidavit (Attachment A) included: a three-page explanation of the offenses under investigation, a seven-page section listing definitions of technical terms used in the affidavit, and a three-page explanation of the Tor network, how it works, and how users could find a hidden service such as "Website A." The affidavit specified the numerous steps a user must go through just in order to find "Website A," because it was a Tor hidden service, and not an ordinary website. In particular, the affidavit at paragraph 10 noted that:

> Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. ["Website A"] is listed in that section.

The experienced affiant accordingly opined that: "Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its purpose and content."

B. Description of "Website A"

The affidavit also described, in great detail, the website whose users were targeted by the investigative technique. It articulated that "Website A" was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while

perpetrating online child sexual exploitation crimes" such as the ones noted in the affidavit. It further articulated that the "administrators and users of the TARGET WEBSITE regularly send and receive illegal child pornography via the website." The affidavit also noted the massive scale of the site, which appeared to have been operating since August of 2014. As of February 3, 2015, site statistics indicated it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.

The affidavit made clear that the illicit purpose was immediately apparent to any user who was able to find the site. As the affiant explained, "on the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." The following text appeared beneath those prepubescent images: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." While those terms may have seemed insignificant to a lay person, the affiant explained, based on his training and his experience, that the phrase "no cross-board reposts" referred to a prohibition against material that is posted on other websites from being "re-posted" to "Website A," and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." The combination of prepubescent images along with these terms of art referencing image posting and large file compression unmistakably marked "Website A" as just what it was—a hub for the trafficking of illicit child pornography images and videos.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site. Users who decided to click on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in the affidavit. That text repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating that "the

forum operators do NOT want you to enter a real [e-mail] address," that users "should not post information [in their profile] that can be used to identify you," that "it is impossible for the staff or the owners of this forum to confirm the true identity of users," that "[t]his website is not able to see your IP," and that "[f]or your own security when browsing on Tor we also recommend that you turn off javascript and disable sending of the 'referer' header." The repeated security warnings of site administration within those registration terms further marked "Website A" as a conduit for illegal activity.

Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail account. Upon successful registration, all of the sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observable. The vast majority of those sections and forums were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. For instance, within the site's "Chan" forum were individual sub-forums for "jailbait" or "preteen" images of boys and girls. There were separate forums for "jailbait videos" and "Jailbait photos" featuring boys and girls. The separate "Pre-teen Videos" and "Pre-teen Photos" forums were each respectively divided into four sub-forums by gender and content, with "hardcore" and "softcore" images/videos separately categorized for boys and girls. A "Webcams" forum was divided into girls and boy's sub-forums. The "Potpurri" [sic] forum contained sub-forums for incest and "Toddlers."

The affidavit described, in graphic detail, particular child pornography that was posted to and available to all registered users of "Website A," that depicted prepubescent females, males, and toddlers, being subjected to sexual abuse and exploitation by adults. Although the affidavit clearly stated that "the entirety of ["Website A" was] dedicated to child pornography," it also

specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children."

The affidavit further explained that "Website A" contained a private messaging feature, which allowed users to send messages directly to one another. The affidavit specified that "numerous" site posts referenced private messages related to child pornography, including an example where one user wrote to another "I can help if you are a teen boy and want to fuck your little sister, write me a private message." According to the affiant's training and experience and law enforcement's review of the site, the affiant articulated his belief that the site's private message function was being used to "communicate regarding the dissemination of child pornography." The affidavit also noted that "Website A" included multiple other features to facilitate the advertisement, distribution, and access to child pornography, including an image host, a file host, and a chat service. All of those features allowed site users to upload, disseminate, and access child pornography. The affidavit contained detailed examples and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features.

C. The Network Investigative Technique

The affidavit contained a detailed and specific explanation of the NIT, indicating why its use was necessary, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.

Specifically, the affidavit noted that without the use of the NIT "the identities of the administrators and users of ["Website A"] would remain unknown" because any IP address logs of user activity on "Website A" would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." Further, because of the "unique nature of the

Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed," whereas the affiant concluded that "using a NIT may help FBI agents locate the administrators and users" of "Website A." The affiant articulated that, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of "Website A" users who were "engaging in the federal offenses enumerated" in the warrant.

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of "Website A" that would be downloaded through normal operation of the site. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. The exact information to be collected was detailed in the warrant, along with technical explanations of the terms. It included the following: (1) an IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) an operating system; (4) information about whether the NIT had already been delivered; (5) a Host Name; (6) an active operating system username; and (7), a Media Access Control (MAC) address. The affidavit explained exactly why the information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." For instance:

> The actual IP address of a computer that accesses ["Website A"] can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

The affidavit specifically requested authority to deploy the NIT each time any user logged into "Website A" with a username and a password. However, the affidavit disclosed to the magistrate that, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation," the FBI might "deploy the NIT more discretely against particular users, including those who "attained a higher status" on the site or "in particular areas of ["Website A"]" such as the sub-forums with the most egregious activity which were described elsewhere in the affidavit. Finally, the affidavit reiterated its specific requests, requesting authority for the NIT to "cause an activating computer—wherever located—to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer."

ARGUMENT

Sullivan does not challenge the accuracy of any of the information articulated by law enforcement in either search warrant. Rather, he raises four arguments regarding the issuance of the NIT search warrant: (1) the warrant was not authorized under Rule 41; (2) a violation of Rule 41 requires suppression; (3) the affidavit failed to establish probable cause because it is not particular; and (4), the good-faith exception does not apply. On those bases, Sullivan contends that evidence seized pursuant to the NIT warrant, and the subsequent warrant executed at his home, should be suppressed. Each of Sullivan's arguments are meritless.

A. The NIT Search Warrant Was Properly Authorized Under Rule 41(b)(4).

Sullivan first argues that since the NIT search warrant was not properly issued, it was void *ab initio*, and therefore, the evidence obtained from that warrant and the subsequent warrant to search Sullivan's home must be suppressed. Reading Rule 41(b) flexibly however, and consistent with how numerous other courts have now found on this very issue, the NIT search warrant was issued in conformity with Rule 41(b)(4).

At the time the NIT search warrant was applied for and obtained, Rule 41(b) of the Federal Rule of Criminal Procedure read as follows in pertinent part:

> Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:
>
> . . . .
>
> (4) *a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device*; *the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both*; . . .
>
> . . . .

Fed. R. Crim. P. 41(b)(4) (emphasis added).

As an initial premise, courts have long read Rule 41 broadly, interpreting it to permit searches that comply with the Fourth Amendment even though not explicitly authorized by the text of the rule. For example, the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact Rule 41's definition of "property" at that time did not include "information," and Rule 41 required that a search be conducted within 10 days. United States v. New York Telephone Co.434 U.S. 159, 169 & n.16 (1977). In so holding, the Supreme Court explained that Rule 41 "*is sufficiently flexible* to include within its scope electronic intrusions authorized upon a finding of probable cause," and

noted that this flexible reading was bolstered by Rule 57(b), which provides, "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." Id. at 169–70 (emphasis added). Similarly, the Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992), opinion corrected (July 16, 1992).

Looking specifically at Rule 41(b)(4), that subsection provides that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). In a typical physical tracking device case, investigators might obtain a warrant to install a tracking device in a container holding contraband. Investigators might then determine the location of the container after targets of the investigation carry the container. The container may very well travel outside the district where the warrant was issued.

In this case, the NIT functioned no differently, except in the more complicated context of dealing with offenders using the internet to commit crimes. Namely, investigators installed the NIT in the Eastern District of Virginia on the server that hosted "Website A." When Sullivan logged on and retrieved information from that server, he retrieved the NIT. The NIT then sent network information, e.g., his IP address, from his computer back to law enforcement. That IP address, that is, "a unique number used by a computer to access the internet," once further

investigated, revealed the physical location of Sullivan's computer vis-à-vis his personally registered internet service.

Seven court decisions have concluded that Rule 41(b)(4) is sufficiently flexible to categorize the NIT as a tracking device, and consequently, they have denied similar motions to suppress. In fact, six of those court decisions pertained to the NIT at-issue in this case. See United States v. Darby, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016); United States v. Matish, No. 4:16-CR-16, 2016 WL 3545776, (E.D. Va. June 23, 2016); United States v. Eure, No. 2:16-CR-43, 2016 WL 4059663 (E.D. Va. July 28, 2016) (incorporating Darby, authored by same judge); United States v. Jean, No. 5:15-CR-50087-001, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); United States v. Smith, No. 15-CR-00467 (S.D. Tex. Sept. 28, 2016); United States v. Dzwonczyk, No. 15-CR-3134 (D. Neb. Oct. 5, 2016) (magistrate's report and recommendation, subject to District Court review); United States v. Johnson, No. 15-CR-00340 (W.D. Mo. Oct. 20, 2016). In the seventh court decision, the District of Nebraska ruled that a similar 2012 NIT warrant was authorized under the tracking device provision of Rule 41(b)(4). See United States v. Laurita, No. 8:13CR107, 2016 WL 4179365 at *6 (D. Neb. Aug. 5, 2016).

Collectively, those seven opinions reasoned that, when the defendant logged into a website like "Website A," he "digitally touched down in," made a "virtual trip," "in essence travelled into the [issuing] district" or "electronically travel[ed]" to the Eastern District of Virginia, where the website was located and in which the NIT was deployed. See Darby, 2016 WL 3189703 at *12; Matish, 2016 WL 3545776 at *18; Laurita, 2016 WL 4179365 at *6; Jean, 2016 WL 4771096 at *17. At that point, the government "installed" the NIT—in the Eastern District of Virginia, which functioned as a tracking device that traveled through the Tor network

and back to the defendant's computer for the purpose of locating it. See Jean, 2016 WL 4771096 at *17 (finding the "NIT was 'install[ed]' for purposes of Rule 41(b)(4), [in] the Eastern District of Virginia, where the tracking device—in this case a string of computer code— was caused to be executed and deployed"). As the Jean court observed:

> The whole point of seeking authority to use a tracking device is because law enforcement does not know where a crime suspect—or evidence of his crime—may be located. In such instances, Rule 41(b)(4) allows a magistrate judge to authorize law enforcement's use of electronic tracking tools and techniques. When an unknown crime suspect, or unknown evidence of his crime, is located in an unknown district, it would be nonsensical to interpret the Rule—as Mr. Jean does—to require law enforcement to make application for such a warrant to an unknown magistrate judge in the unknown district. The fact that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return location identifying information from outside the Eastern District of Virginia—is not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception.

Jean, 2016 WL 4771096 at *17.

Here, Sullivan did in fact take action to control the government-controlled computer—the "Website A" server—by requesting that computer to deliver information to him. Moreover, the "property" tracked was the information stored on the "Website A" server, which was requested by and sent to him. In other words, the NIT tracked where the content sent through Tor went and then let law enforcement know where it landed. This argument is further supported by Rule 41's text, which defines "property" to include "information." Rule 41(a)(2)(A). This view is also supported by the NIT warrant itself, which specified that, during the course of normal operation, "websites send content to visitors," "a user's computer downloads that content and uses it to display web pages on the user's computer," the NIT "would augment that content with additional computer instructions . . . which comprise the NIT," and that those instructions are "designed to cause the user's 'activating' computer to transmit certain information" to a

government computer, which would "assist in identifying the user's computer, its location, and the user of the computer."

Also case, it was Sullivan who, on multiple occasions reached out to the Eastern District of Virginia, and unwittingly carried the NIT back with him to Painesville, Ohio—along with the rest of the "Website A" content he accessed and sought. Therefore, Sullivan's own actions illustrate how "installation" in Eastern District of Virginia occurred in accordance with Rule 41(b)(4). That the NIT would only return information after it reached its ultimate destination, Sullivan's computer, should not necessarily be determinative—especially in this advanced era of internet, deep net, Tor, exit nodes, hidden websites, encryption, etc.—all pieces of information that committees writing and revising Rule 41 could have never possibly envisioned or anticipated.

On December 1, 2016, subsection (b)(6) was added to Rule 41. In pertinent part, Subsection (b)(6) states:

> At the request of a federal law enforcement officer or an attorney for the government, . . . a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means . . . .

By enactment of this subsection, Sullivan argues that (b)(6) is an *ipso facto* concession that (b)(4) did not provide the United States magistrate judge with authority to issue the NIT warrant. He attaches to his motion and essentially apes the court's opinion and order in United States v. Levin, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016). However, Levin is non-binding legal precedent, wherein that court found the NIT warrant, without

explanation, not a "tracking device" under any circumstance. Levin remains a minority position of the courts involved in "Website A" litigation past and present.[3]

Further, the newly enacted Rule 41(b)(6) neither retroactively negated the explicit authority of (b)(4), nor was (b)(4) expressly amended to exclude remote access warrants from the umbrella from which seven courts have determined them to be "tracking devices." Rather, (b)(6) was crafted merely to eliminate any ambiguity as to a magistrate judge's Rule 41 authority to issue warrants in this ever-growing technological world. Likewise, the rule was crafted because its drafters couldn't have foreseen the potential for child predators like Sullivan to utilized a "deep net" site such as Tor to mask their pedigree and location data—data necessary to aid in their capture. Finally, the rule was crafted to address a non-unanimous judiciary's interpretation of Rule 41(b)(4) as to whether a remote access of electronic storage media, e.g., NITs, qualify as tracking devices. (A non-unanimous judiciary whose majority has concluded that NITs fall within the (b)(4) definition of a "tracking device," and where the minority opinions are one-by-one now pending appeal.)

In conclusion, interpreting Rule 41 flexibly, and finding consistent with sister courts that the NIT qualified as a tracking device under Rule 41(b)(4), is entirely appropriate. Conversely, a rigid interpretation of Rule 41 would lead to courts denying magistrates the authority to issue warrants otherwise consistent with the Fourth Amendment, due solely to the fact that they do not fit neatly into Rule 41's parameters. Such a rigid interpretation does not account for advances in

[3] In fact, since May 5, 2016 when Levin's Opinion and Order was published, three other courts in the District of Massachusetts in part disagreed with Levin and held the NIT warrant not subject to suppression. See United States v. Anzalone, No. 15-CR-10347, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); United States v. Allain, No. 15-CR-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); United States v. Stepus, No. 15-CR-30028 (D. Mass. Oct. 28, 2016). In addition, the United States appealed Levin's findings and rulings to the First Circuit to revisit. See United States v. Levin, No. 16-1567 (1st Cir. Oct. 26, 2017) (Westlaw cite not available).

technology; likewise, such a rigid interpretation would unnecessarily encourage warrantless searches justified by claims of exigency. See United States v. Torres, 751 F.2d 875, 880 (7th Cir. 1984) ("A holding that federal courts have no power to issue warrants authorizing [an investigative technique] might . . . simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment."). Finally, the 2006 Amendments to Rule 41(b), which added Rule 41(b)(4), also reflect a preference for judicial approval of warrants based on new tracking technology.

For all of the above reasons, the NIT search warrant was properly authorized under Rule 41, because Rule 41(b) is flexible enough to allow for the issuance of warrants to investigate Tor hidden services like "Website A," and because the NIT acted as a tracking device under Rule 41(b)(4) that surreptitiously captured Sullivan's criminal acts.

B. Any Purported Violation of Rule 41 Does Not Require Suppression

Sullivan next argues that since Rule 41 was violated at the time the NIT search warrant was obtained, suppression is required due to the United States' lack of compliance. He claims that but-for the NIT search warrant, he would have never suffered prejudice. Here, the prejudice he suffered was the subsequent search of his home that might never have occurred, or a search would not have been so abrasive. Sullivan makes these blanket assertions without explanation.

Assuming *arguendo* that this Court finds that the NIT warrant was not properly issued under Rule 41, as an initial premise, suppression of evidence derived from a search warrant is a "last resort," not a "first impulse." Herring v. United States, 555 U.S. 135, 140 (2009). And any benefit to doing so, e.g., general deterrence of law enforcement misconduct, must outweigh the substantial social cost that results when "guilty and possibly dangerous defendants go free." Id.

at 140–41. Accordingly, defendants who seek suppression must clear a "high obstacle," id. at 141, and "resolution of doubtful or marginal cases . . . should largely be determined by the preference to be accorded to warrants." United States v. Kelley, 482 F.3d 1047, 1050–51 (9th Cir. 2007) (citing and quoting Illinois v. Gates, 462 U.S. 213, 237 n.10 (1983)).

Applying Herring, the Sixth Circuit recently addressed an instance where evidence was derived from an improperly issued warrant. In United States v. Master, 614 F.3d 236 (6th Cir. 2010), a sheriff's investigator obtained a warrant from a Franklin County, Tennessee state judge. However, it was later learned that the target residence was actually located in Coffee County, Tennessee, and therefore, the Franklin County judge lacked the authority to issue the warrant to search at Masters' residence. Despite finding that the search violated Masters' Fourth Amendment rights, the Sixth Circuit upheld the admission of evidence derived from that warrant. In so holding, it offered the below rationale:

> The Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, "the benefits of deterrence must outweigh the costs." In following the Supreme Court's approach with respect to the instant case, the costs of excluding the evidence would appear to outweigh any deterrent effect. This is so, in no small measure, because the Herring Court's emphasis seems weighed more toward preserving evidence for use in obtaining convictions, even if illegally seized, than toward excluding evidence in order to deter police misconduct unless the officers engage in "deliberate, reckless, or grossly negligent conduct."

Id. at 243 (citations omitted).

At best, the issuance of the NIT warrant by an Eastern District of Virginia magistrate judge was merely technical—not deliberate, reckless, or grossly negligent conduct. The NIT search warrant was issued by a neutral magistrate judge. It was based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense." And as discussed later, the NIT warrant met the particularity requirement.

Moreover, the United States' actions here were entirely reasonable under the circumstances. Law enforcement clearly had a substantial interest in identifying users of a massive website trafficking in child pornography. The court-authorized use of the NIT was necessitated by the Tor-based technology Sullivan and other offenders hid behind to exploit children. That technology, without use of the NIT, made it impossible for law enforcement to know who Sullivan was and from where he was physically hiding while sexually exploiting children.

The individual privacy interests here were also extremely limited, due to the minimally invasive nature of the NIT search and its focus on IP address information. Notably, Sullivan's IP address didn't even belong to him, and so he didn't even have a reasonable expectation of privacy in the IP address that ultimately led to his identification. See United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (internet users have no expectation of privacy in the IP addresses of the websites they visit); see also Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (defendant has no Fourth Amendment right in subscriber information provided to an internet provider).

Finally, before proceeding with a more invasive entry and search of Sullivan's home and the electronic devices found therein, the United States obtained a second search warrant issued in this district. The very fact the United States sought and obtained a second warrant from a neutral magistrate judge protected Sullivan from an unreasonable search and seizure in violation of his constitutional rights. See United States v. Alvarez, 810 F.2d 879, 883 (9th Cir. 1987) (interposing magistrate judge between law enforcement and target protects against unreasonable searches).

Consistent with the aforementioned law and analysis, seventeen courts ruled that although the at-issue NIT search warrant was not properly issued pursuant to Rule 41, suppression is unwarranted. See United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); United States v. Stamper, No. 1:15cr109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); United States v. Epich, No.15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016) (unnecessary to reach the issue of Rule 41 compliance, suppression unwarranted); United States v. Werdene, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); United States v. Rivera, No. 2:15-CR-266-CJB-KWR (E.D. La. Jul. 20, 2016); United States v. Acevedo-Lemus, No. 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); United States v. Adams, No. 16-CR-011 (M.D. Fl. Aug. 10, 2016); United States v. Torres, No. 16-CR-285, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); United States v. Henderson, No. 15-CR-565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); United States v. Scarbrough, No. 16-CR-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016) (adopting Mag. Rep. and Rec.); United States v. Knowles, No. 15-CR-875 (D. S.C. Sept. 14, 2016); United States v. Ammons, No. 3:16-CR-00011, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); United States v. Broy, No. 16-CR-10030, 2016 WL 5172853 (C.D. Ill. Sept. 21, 2016); United States v. Anzalone, No. 15-CR-10347, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); United States v. Allain, No. 15-CR-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); United States v. Libbey-Tipton, No. 16-CR-236 (N.D. Ohio Oct. 19, 2016);[4] United States v. Stepus, No. 15-CR-30028 (D. Mass. Oct. 28, 2016); but see Levin, 2016 WL 2596010; United States v. Arterbury, No. 15-CR-182-JHP (N.D. Okla. May 17, 2016); United States v. Workman, No. 15-CR-397 (D. Colo. Sept. 6, 2016); United States v.

[4] Like Levin, the United States filed an appeal now pending circuit court consideration. See United States v. Workman, No. 16-1401 (10th Cir. Dec. 28, 2016) (Westlaw cite not yet available).

Croghan (and Horton) (consolidated order), Nos. 15-CR-48;15-CR-51, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016)[5] (all finding issuing magistrate lacked jurisdiction under Rule 41 to issue NIT warrant requiring suppression).

In Libbey-Tipton, a Northern District of Ohio sister court held that suppression was not warranted. In ruling consistent with the overwhelming majority of the other courts to have visited this very same issue, it explained:

> If the government's case is proven, however, defendant engaged in the downloading of child pornography on a number of occasions and took measures specifically designed to avoid detection. It is obvious that the cost of excluding the evidence is substantial. On the other hand, the Court finds a negligible, if any, deterrent effect on the conduct of law enforcement. . . . Here, the Court finds that suppression is unwarranted. To do so would cause the exclusion of reliable evidence bearing on guilt or innocence in exchange for little or no deterrent effect.

Libbey-Tipton, No. 16-CR-236, *11–12.

In conclusion, assuming there was a technical violation of Rule 41, that violation does not warrant suppression. The NIT search warrant was reasonable in its scope, it was supported by ample probable cause, there is absolutely no evidence of overreach or abuse committed by law enforcement, and any intrusion to Sullivan's privacy rights was minimal. Applying Masters, 614 F.3d at 243, "the benefits of deterrence" do not "outweigh the costs"—suppression in this case is clearly unwarranted.

C. The NIT Search Warrant Was Sufficiently Particular

Sullivan next contends that the NIT warrant failed to particularly describe the place to be searched. He bases his argument solely on the fact that the NIT warrant did not expressly

[5] Like Levin, the United States filed an appeal now pending circuit court consideration. See United States v. Horton (& Croghan), Nos. 16-3976 (L) & -3982, 2016 WL 6905741 (8th Cir. Nov. 22, 2016).

mention Sullivan's Painesville home.[6] He does not argue that the NIT warrant itself failed to particularly describe the items to be seized.

The Fourth Amendment requires that a warrant describe with "particular[ity] . . . the place to be searched and the persons or things to be seized." U.S. Const., Amend. IV. "It is enough if the description is such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended." Steele v. United States, 267 U.S. 498, 503 (1925). Likewise, "The Fourth Amendment . . . does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed] in the warrant: 'the place to be searched 'and 'the persons or things to be seized.'" United States v. Grubbs, 547 U.S. 90, 97 (2006) (citing Dalia v. United States, 441 U.S. 238, 257 (1979)). There is no legal requirement that a search warrant specify the precise manner in which the search is to be executed. Dalia, 441 at 257; see also United States v. Rigmaiden, No. 08-CR-814, 2013 WL 1932800, at *16 (D. Ariz. May 8, 2013) (rejecting argument that tracking warrant was insufficiently particular even where warrant did not describe "the precise means by which the . . . device would operate."). Finally, a warrant may be issued when there is probable cause to search for and seize evidence of crime, even if "the owner or possessor of the place to be searched is not then reasonably suspected of criminal involvement." Zurcher v. Stanford Daily, 436 U.S. 547, 560 (1970).

Here, Attachments A and B of the NIT warrant, entitled "Place to be Searched," and "Information to be Seized," aptly describe with precise language exactly what would be searched and seized. Namely, the warrant authorized the NIT to be deployed on the computer server

[6] Of course, this type of circular argument further supports this Court's flexible read of Rule 41(b)(4), since without the NIT warrant, law enforcement could never learn the location of Sullivan's Painesville, OH home address.

hosting "Website A," in order to obtain specific information from computers of "any user or administrator who logs into ["Website A"] by entering a username and password." The "specific information" was detailed in Attachment B, and included: the computer's actual IP address, and the date and time that the NIT determines what that IP address is; a unique identifier generated by the NIT to distinguish data from that of other computers; the type of operating system running on the computer; information about whether the NIT has already been delivered to the "activating" computer; the computer's Host Name; the computer's active operating system username; and the computer's media access control ("MAC") address.

Consistent with Supreme Court precedent and after analyzing the aforementioned facts, the same seventeen courts that found any Rule 41 violation merely technical and suppression unwarranted also found the NIT warrant sufficiently particular. See Michaud, 2016 WL 337263, at *5; Stamper, 2016 WL 695660, at *19; Epich, 2016 WL 953269, at *2; Darby, 2016 WL 3189703, at *8; *Matish*, 2016 WL 3545776, at *14; Rivera, No. 2:15-CR-266-CJB-KWR, at 11–13; Acevedo-Lemus, 2016 WL 4208436, at *7 n.4; Henderson, 2016 WL 4549108, at *4; Jean, 2016 WL 4771096, at *11–12; Knowles, No. 15-CR-875, at 22–23; Broy, 2016 WL 5172853, at *3; Anzalone, 2016 WL 5339723, *7; Smith, No. 15-CR-00467, at 8; Allain, 2016 WL 5660452, at *8–9; Dzwonczyk, No. 15-CR-3134, at 15; Scarbrough, 2016 WL 5900152, at 14; Johnson, No. 15-CR-00340, at 6.

In Broy, that Court—in an all-encompassing fashion, directly addressed Sullivan's sole basis for claiming a lack of particularity,

> That the warrant encompassed a large number of possible computers potentially located in a large number of districts does not mean it suffered from a lack of particularity; it merely indicates the FBI suspected a large number of users would access Website A from all over the country . . . [and] the warrant listed the seven specific pieces of information the NIT would gather from the activating computer

> and send back to the government computer in the Eastern District of Virginia . . . [t]hus both the place and items to be seized were described with sufficient particularity so as not to render the warrant a general one.

Broy, 2016 WL 5172853, at *3.

In Michaud, that Court further elaborated its particularity finding in the context of the massive criminal enterprise the online "Website A" presented:

> The NIT Warrant does not, however, lack sufficient specificity. The warrant states with particularity exactly what is to be searched, namely, computers accessing Website A. According to the warrant application upon which the NIT Warrant was issued, Website A is unmistakably dedicated to child pornography. Although the FBI may have anticipated tens of thousands of potential suspects as a result of deploying the NIT, that does not negate particularity, because it would be highly unlikely that Website A would be stumbled upon accidentally, given the nature of the Tor network.

Michaud, 2016 WL 337263, at *5.

Concluding, the omission of Sullivan's Painesville, OH home from the NIT warrant is immaterial. The NIT warrant was sufficient particular in the places to be searched and the things it was to seize.

D. The Good-Faith Exception Applies

Finally, Sullivan argues that since the NIT search warrant exceeded judicial authority, it violated Sullivan's Fourth Amendment rights and therefore the good-faith exception does not apply.

Again, assuming *arguendo* that this Court were to find that the evidence was improperly seized pursuant to the NIT search warrant and subsequent search warrant, the evidence is still admissible under the good-faith exception to the exclusionary rule. In United States v. Leon, 468 U.S. 897 (1984), the Supreme Court held that in the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were

dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause. Id. at 926. Such determinations must be made on a case-by-case basis with suppression ordered" only in those unusual cases in which exclusion will further the purpose of the exclusionary rule." Id. at 918. Seeking a search warrant is prima facie evidence that the officer was acting in good faith. United States v. Mitten, 592 F.3d 767, 771 (7th Cir. 2010).

The Supreme Court found that reliance on an invalid search warrant would not be reasonable if: (1) the affidavit included information the officer knew was false or would have known to be false except for the officer's reckless disregard for the truth and such information misled the issuing magistrate; (2) the issuing magistrate abandoned a neutral and detached role; (3) the warrant was based on an affidavit with so few indicia of probable cause that an objective belief in its validity would be unreasonable; and (4), the warrant itself was so facially deficient that the executing officers could not rely upon its validity.

None of the exceptions set forth in Leon apply in this case. Sullivan does not contend, nor does he cite to any evidence, that either magistrate judge who approved warrants pertinent to his case abandoned their neutral and detached roles. Sullivan also makes no allegation that any of the information articulated in either warrant was dishonest or reckless. Further, as noted herein, the comprehensive 31-page NIT affidavit amply articulated probable cause for the requested technique. Accordingly, the court should find that all of the evidence Sullivan requests the court to suppress is admissible pursuant to the good-faith exception.

CONCLUSION

For all of the above reasons, the United States respectfully requests that this court deny the defendant's Motion to Suppress. The United States believes oral argument is unnecessary and relies on this written response in opposition to Sullivan's motion.

Respectfully submitted,

CAROLE S. RENDON
United States Attorney

By: */s/ Benedict S. Gullo*
Benedict S. Gullo (NY: 3013570)
Assistant U.S. Attorney
Suite 400, U.S. Courthouse
801 West Superior Avenue
Cleveland, Ohio 44113–1852
Tel. No. (216) 622-3807
E-mail: benedict.gullo@usdoj.gov

CERTIFICATE OF SERVICE

I certify that on January 5, 2017, a copy of the foregoing United States of America's Sentencing Memorandum was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt.

/s/ Benedict S. Gullo
Assistant U.S. Attorney